UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/580,689	05/30/2000	Arturo Maria	113639	1763

24197 7590 05/30/2006

KLARQUIST SPARKMAN, LLP
121 SW SALMON STREET
SUITE 1600
PORTLAND, OR 97204

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/580,689	MARIA, ARTURO	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-14,23-30 and 32-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-14,23-30 and 32-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 May 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 3/3/2006, Applicant amends claims 1, 5, 7, 12, 23, 30, 32, and cancels claims 15-22 and 31. The following claims 1-5, 7-14, 23-30, and 32-38 are presented for examination.

2. Applicant's arguments, pages 6-10, filed on 3/3/2006, with respect to the rejection of claims 1-5, 7-30, and 32-38 have been fully considered but they are not persuasive. Applicant has amended the independent claims to recite plurality of computers instead of a computer. Applicant erroneously argues that Yavatkar does not teach or suggest installing intrusion detection services on plurality of computers and executing detection services on a plurality of computers but Yavatkar instead teaches installing intrusion detection services only at an active device that is close to the location of the intrusion. Examiner respectfully disagrees. Yavatkar states, "we describe in this article Intel's framework for programmable networks. The objective of the Phoenix framework is to make it easier to deploy new network services that leverage the emerging trend toward use of reprogrammable network processors" (see abstract). "The Phoenix framework defines a mobile agent system that allows an agent to be launched into the network to visit active devices and manipulate proactive service... the network administrators use the proactive consoles to install a new proactive service on active devices..." (see page 161, paragraphs 3-5). With respect to the dependent claims, applicant erroneously states claims 5, 12, 18, 26 and 27 are rejected under 103 whereas claim 37 instead of claim 27 is rejected under 103.

Applicant adds that claim 18 is cancelled without prejudice; it appears that applicant concedes that Yavatkar discloses the limitation of claim 18. Applicant argues about claim 37, while claim 18 and claim 37 disclose similar limitations (a stop condition that is an expiration time). Applicant erroneously states that claim 5 has been amended to recite wherein the stop condition is an expiration time of a request to initiate intrusion, which is not recited in the claim nor in the specification. It is also noted that the original specification and the original claims disclose a stop condition indicating when to stop intrusion detection services wherein the stop condition is an expiration time but do not disclose expiration time of a request nor expiration time of a request to initiate intrusion. In response to applicant's arguments that the prior art does not disclose a stop condition (when to terminate) related with time, Yavatkar discloses instantiate start and stop process of intrusion detection services which implicitly includes time to start and stop and Porras further discloses monitoring events in time domain to produce responses and countermeasures as further explained below. Upon further consideration, applicant has not overcome the rejection of claims claims 1-5, 7-14, 23-30, and 32-38 by amending the claims, and the claims remain rejected in view of the same references.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 5 and 12 are rejected under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as their invention. Evidence that claims 5 and 12 fail(s) to correspond in scope with that which applicant(s) regard as the invention can be

found in the reply filed 3/3/2006. In that paper, applicant has stated wherein the stop condition is an expiration time of a request to initiate intrusion, and this statement indicates that the invention is different from what is defined in the claim(s) because the original specification and the original claims merely disclose monitoring a stop condition indicating when to stop or terminate intrusion detection services wherein the stop condition is an expiration time. The original specification does not disclose expiration time of a request nor expiration time of a request to initiate intrusion.

Claim Rejections - 35 USC § 102

4. (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4.1 **Claims 1-4, 7-11, 13-17, 19-25, 27-36, and 38** are rejected under 35 U.S.C. 102(a) as being anticipated by Non-Patent Literature by Raj Yavatkar, David Putzolu, Sanjay Bakshi, Satyendra Yadav, "The Phoenix Framework: A Practical Architecture for Programmable Networks"; March 2000; IEEE Communications Magazine; Pages 160-165.

4.2 **As per claims 1 and 30, Yavatkar et al** discloses a method for implementing an intrusion detection system in a network, comprising receiving a request at a software agent program to initiate intrusion detection services on a plurality of remote computers wherein the request is issued in response to a notification of a network intrusion, for example (see page 165,

first column; see also page 163, second column, emphasis added, network contains several switches, routers, and PCs or active devices, launching and controlling application on each PC); and discloses the launching of mobile agent which also can install code into the device that meets the recitation of installing intrusion detection software on said remote computer via said software agent program, for example (see page 165, first column) and executing said intrusion detection software on said remote computer via said software agent program, for example (see page 165, first column and conclusion) **Yavatkar et al** in one embodiment uses one device as an example to illustrate the process or uses a device as a proxy. However, **Yavatkar et al** discloses request at a software agent program to initiate intrusion detection services on a plurality of computers (see page 161, paragraphs 3-5 and abstract). Page 162 cites agents can install services at the device itself or other active device acting as proxy, therefore services may be installed at each device from a plurality of eligible devices... agent carries a policy that defines conditions that determine whether or not each device should execute a software, **Yavatkar et al** provides additional disclosure on page 161 about installing and executing intrusion detection software on a remote computer. Page 164, second column and page 163, second column disclose installation request in response to network attacks and to alleviate congestion.

As per claim 23, Yavatkar et al discloses a system for detecting intrusions in a computer network comprising: a plurality of computers executing software agents (page 162, column 2: configuration); an intrusion detection server (see figure 4) any network device can be acted as an instruction server without departing from the spirit and scope of the invention disclosed by **Yavatkar et al**; and a database configured to store at least one rule defining at least

one response to a network intrusion, wherein said intrusion detection server is configured to send a request to execute intrusion detection software to software agents at a plurality of computers when intrusion detection services are needed based on the at least one rule stored in said database (see page 162 and page 165, first column). Page 163, second column discloses several PCs or active devices used by agents to perform variety of tasks such as monitoring, configuration, launching, etc.

As per claim 2, Yavatkar et al discloses that third parties can request mobile agents to start, suspend, stop, and destroy services that meets the recitation of receiving a request to terminate intrusion detection services at said software agent program (see page 161, second column).

As per claims 3 and 20, Yavatkar et al discloses the limitation of monitoring for fulfillment of a stop condition (see congestion analysis, page 164 *with emphasis on second column, first paragraph)*.

As per claims 4, 13, 19, and 38, Yavatkar et al discloses the limitation of wherein said stop condition is based on network traffic conditions (see congestion analysis, page 164 *with emphasis on second column, first paragraph)*.

As per claims 7 and 32, Yavatkar et al discloses the limitation of selecting said remote computers from a plurality of eligible computers (see page 162, second column and page 165, first column).

As per claims 8 and 33, Yavatkar et al discloses the limitation of wherein said selecting step is accomplished based on a network physical topology of the network that meets the recitation of said selecting step is accomplished based on a network map (page 162 and page 165, first column).

As per claims 9, 29, and 34, Yavatkar et al discloses the limitation of wherein said selecting step is accomplished based on a knowledge base (page 162, second column, paragraphs 1 and 2).

As per claims 10, 14, and 35, Yavatkar et al discloses security services for agent authentication authentication and authority that meets the limitation of wherein said request is verified using a cryptographic authentication scheme (page 161, column 2: proactive services).

As per claims 11 and 36, Yavatkar et al discloses the limitation of wherein said request includes a stop condition indicating when to stop executing the intrusion detection software program, for example (see page 161, second column).

As per claim 24, Yavatkar et al discloses the limitation of wherein said intrusion detection server increases the number of said plurality of computers executing intrusion detection software when a network intrusion is detected (see page 162).

As per claim 25, Yavatkar et al discloses the limitation of wherein said intrusion detection server changes the number of said plurality of computers executing intrusion detection software when the level of network traffic changes (see page 162).

As per claim 27, Yavatkar et al discloses the limitation of wherein said database contains information about the plurality of computers (see page 162).

As per claim 28, Yavatkar et al discloses the limitation of wherein said information includes a map of said computer network (page 162 and page 165, first column).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject

matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.1 **Claims 5, 12, 26, and 37** are rejected under 35 U.S.C. 103(a) as being unpatentable over Raj Yavatkar, David Putzolu, Sanjay Bakshi, Satyendra Yadav, "The Phoenix Framework: A Practical Architecture for Programmable Networks"; March 2000; IEEE Communications Magazine; Pages 160-165, in view of US Patent 6,484,203 to **Porras et al**.

5.2 **As per claims 5 and 12, Yavatkar et al** substantially discloses automatic deployment of network services (see abstract) and monitoring stop condition with respect to network traffic, and further discloses the framework provides basic intrusion detection services used by agent to instantiate start, suspend, stop and destroy services (see page 161, second column), but does not explicitly disclose wherein said stop condition is an expiration time. However, it is well known to one of ordinary skill in the art that network entities can be scheduled to dynamically instantiate start, suspend, stop of intrusion detection services. **Porras et al** in an analogous art teaches an event monitoring and analysis for network intrusion system, identifying attacks in plurality of network entities, detecting network intrusions based on analysis of network traffic, generating reports of suspicious activity, (see column 1, line 50 through column 2, line 22) and a response method that include threshold metric based on the associated attacks (column 11, lines 15-31); the monitors may distinguish between normal data transfer during a workday and abnormal data transfer during a weekend evening (column 12, lines 23-40 and column 5, lines 21-45). Monitors can help domains counter the attack and can sensitize other domains to such

attacks before they are affected (column 3, lines 55-66). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Yavatkar et al** to provide monitoring of start and stop condition of intrusion detection services based on expiration time as taught by **Porras et al**. This modification would have been obvious because **Yavatkar et al** discloses that the framework provides basic services used by agent to instantiate start, suspend, stop and destroy services (see page 161, second column) and discloses temporarily stopping service on a router as to use another active device (page 165, 2nd paragraph) and as **Porras et al** discloses monitoring traffic volume in intrusion detection system, generating results that network failure of specific network entity may occur at specific time of day due to traffic rate; for instance, network traffic at 11:00 am is much different than midnight, and producing countermeasures based on the reports, (column 12, lines 18-40 and column 5, lines 21-45) one of ordinary skill in the art would have been motivated by the above suggestions to monitor when to start/stop network services based on time of day because specific day and time are more subject to network attacks and network congestion than others.

As per claim 37, Yavatkar et al substantially discloses automatic deployment of network services (see abstract) and monitoring stop condition with respect to network traffic, and further discloses the framework provides basic services used by agent to instantiate start, suspend, stop and destroy services (see page 161, second column), but does not explicitly disclose wherein said stop condition is an expiration time. However, it is well known to one of ordinary skill in the art that network entities can be scheduled to dynamically instantiate start, suspend, stop of intrusion detection services. **Porras et al** in an analogous art teaches an event

monitoring and analysis for network intrusion system, identifying attacks in plurality of network entities, detecting network intrusions based on analysis of network traffic, generating reports of suspicious activity, (see column 1, line 50 through column 2, line 22) and a response method that include threshold metric based on the associated attacks (column 11, lines 15-31); the monitors may distinguish between normal data transfer during a workday and abnormal data transfer during a weekend evening (column 12, lines 23-40 and column 5, lines 21-45). Monitors can help domains counter the attack and can sensitize other domains to such attacks before they are affected (column 3, lines 55-66). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Yavatkar et al** to provide monitoring of start and stop condition of intrusion detection services based on expiration time in order to manage a channel synchronization between the devices and monitor connection failure as taught by **Porras et al**. This modification would have been obvious because **Yavatkar et al** discloses that the framework provides basic services used by agent to instantiate start, suspend, stop and destroy services (see page 161, second column) and discloses temporarily stopping service on a router as to use another active device (page 165, 2nd paragraph) and as **Porras et al** discloses monitoring traffic volume in intrusion detection system, generating results that network failure of specific network entity may occur at specific time of day due to traffic rate; for instance, network traffic at 11:00 am is much different than midnight, and producing countermeasures based on the reports, (column 12, lines 18-40 and column 5, lines 21-45) one of ordinary skill in the art would have been motivated by the above suggestions to monitor when to start/stop network services based on time of day because specific day and time are more subject to network attacks and network congestion than others.

As per claim 26, Yavatkar et al substantially discloses providing new network resources as required to take action to alleviate congestion (page 164). **Porras et al** refers to time of day when network traffic is heavier than other time of day (column 5, lines 22-45). Monitors can help domains counter the attack and can sensitize other domains to such attacks before they are affected (column 3, lines 55-66). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Yavatkar et al** to have the intrusion detection server changed the number of said plurality of computers executing intrusion detection software depending on the time of day as suggested by both references. This modification would have been obvious because **Yavatkar et al** discloses once an administrator has reviewed information gathered from network analysis they can take action to alleviate congestion by reconfiguring, applying some sort of traffic shaping behavior based on the underlying causes of network congestion or provisioning new network resources as required (page 164, second column) and as Porras et al discloses monitoring traffic volume in intrusion detection system, generating results that network failure of specific network entity may occur at specific time of day due to traffic rate; for instance, network traffic at 11:00 am is much different than midnight, (column 12, lines 23-40 and column 5, lines 21-45) and producing countermeasures based on the reports, one of ordinary skill in the art would have been motivated by the above suggestions to provide more network resources based on time of day where congestion is much heavier.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

6.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin
Patent Examiner
May 25, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100